MODERN MANAGEMENT REVIEW **2017**
MMR, vol. XXII, 24 (2/2017), pp. 117-130 **April-June**

Stanisław J. RYSZ[1]

INTEGRACJA INFORMATYCZNA W OBSZARZE ZARZĄDZANIA KRYZYSOWEGO

Specyfika zarządzania kryzysowego polega w dużej mierze na poszukiwaniu możliwości ograniczania skutków zdiagnozowanych zagrożeń oraz na podążaniu z akcjami reagowania do miejsc ich materializacji. Idąc dalej w tych rozważaniach trzeba dostrzec, że pakietowość występujących zagrożeń, ich nieprzewidywalność zarówno co do charakteru, jak i co do skali sprawiają, że koszty działań zawsze przerastają zaplanowane na ich realizację środki budżetowe. Trzeba więc szukać sposobów, żeby ta dysproporcja była jak najmniejsza. Służyć temu mogą informatyczne systemy integrujące zasoby procesu zarządzania kryzysowego. Środowisko podmiotów uczestniczących w systemie zarządzania kryzysowego w Polsce ma charakter hybrydowego klastra. Oprócz organów administracji publicznej, służb, straży i inspekcji, które są do tego zobligowane zapisami odpowiednich ustaw, uczestniczą w nim także podmioty komercyjne (działające dla osiągnięcia zysku) oraz organizacje społeczne z tak zwanego trzeciego sektora. Taka specyfika uczestników naraża system na trudności w godzeniu partykularnych interesów poszczególnych podmiotów, co może utrudniać uzyskanie optymalnej sprawności i skuteczności. Z uwagi na istotne znaczenie dostępności i przepływu informacji w procesach zarządzania kryzysowego, można się spodziewać, że wdrożenie informatycznych narzędzi i procedur integrujących środowisko może mieć pozytywny wpływ zminimalizowanie takich zagrożeń. Chodzi o zorganizowanie współpracy w środowisku podmiotów działających w systemie zarządzania kryzysowego poprzez wykorzystanie zasobów informatycznych i teleinformatycznych (sprzętowych, aplikacyjnych, sieciowych i personalnych) do sprawniejszego pozyskiwania danych niezbędnych do właściwej oceny przebiegu zdarzeń, inwentaryzacji dostępności i zużycia zasobów oraz planowania i prowadzenia akcji w sytuacjach kryzysowych.

Słowa kluczowe: zarządzanie kryzysowe, integracja, sprawność, skuteczność.

1. WSTĘP

Do uzasadnienia potrzeby optymalizowania struktur i działań systemu zarządzania kryzysowego w Polsce najlepszych argumentów dostarcza rachunek ekonomiczny. Pieniądze widziane z perspektywy płatnika mają oprócz wartości nabywczej jeszcze ten atrybut, że wydawane kiedyś się kończą. Poza tym, wobec permanentnego stanu, kiedy potrzeby finansowe istotnie przewyższają dostępność środków, konieczne jest odpowiednie i odpowiedzialne nimi gospodarowanie. Chodzi nie tylko o próby zapewniania (zwiększania) odpowiednich kwot na funkcjonowanie i modernizację systemu zarządzania kryzysowego, ale

[1] Dr Stanisław J. Rysz – w latach 2008–2016 zastępca dyrektora Wydziału Bezpieczeństwa i Zarządzania Kryzysowego Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie. Autor kilkudziesięciu artykułów i kilku monografii z obszaru nauk o bezpieczeństwie, wykładowca Politechniki Rzeszowskiej, Uniwersytetu Rzeszowskiego, WSPiA Rzeszowskiej Szkoły Wyższej; e-mail: stanislaw.rysz@vp.pl.

przede wszystkim o wprowadzenie w nim takich zmian i innowacji, które sprawią, że dostępne środki będą lepiej wykorzystywane[2].

Celem artykułu jest ukazanie możliwości optymalizacji funkcjonowania zarządzania kryzysowego w Polsce poprzez wdrożenie w nim zintegrowanego systemu informatycznego.

2. WPROWADZENIE DO ROZWAŻAŃ

Środowisko podmiotów powołanych i planowanych do udziału w systemie zarządzania kryzysowego w Polsce ma charakter hybrydowego klastra[3]. Uczestniczą w nim oprócz organów administracji publicznej, służb, straży i inspekcji, które są do tego zobligowane zapisami odpowiednich ustaw, także podmioty komercyjne (działające dla osiągnięcia zysku[4]) oraz organizacje społeczne z tak zwanego trzeciego sektora[5]. Taka specyfika elementów systemu zarządzania kryzysowego dopuszcza możliwość występowania trudności w godzeniu partykularnych interesów poszczególnych podmiotów i uzyskaniu optymalnej sprawności i skuteczności prowadzonych przez nie działań w ramach systemu.

Z uwagi istotne znaczenie dostępności i przepływu informacji w procesach zarządzania kryzysowego, można się spodziewać, że wdrożenie w systemie informatycznych narzędzi i procedur integrujących środowisko może mieć pozytywny wpływ na jego funkcjonowanie. Chodzi o to, żeby dokonać integracji środowiska podmiotów działających w systemie zarządzania kryzysowego poprzez wykorzystanie zasobów zasoby informatycznych i teleinformatycznych (sprzętowych, aplikacyjnych, sieciowych i personalnych) do sprawniejszego pozyskiwania danych niezbędnych do właściwej oceny przebiegu zdarzeń, inwentaryzacji dostępności i zużycia zasobów oraz planowania i prowadzenia akcji w sytuacjach kryzysowych.

Zagadnienie z pozoru wydaje się jasne i proste – tylko brać i działać, jednak po głębszej jego analizie pojawia się kilka obszarów, które wymagają szczególnego zainteresowania i podejścia z zachowaniem najwyższych standardów.

Integracja powinna przebiegać z uwzględnieniem uwarunkowań nowego, globalnego środowiska przetwarzania, które powstało i rozwija się dzięki włączaniu się kolejnych podmiotów i ich systemów za pomocą sieci teleinformatycznych. Działania integracyjne mają coraz częściej charakter międzyorganizacyjny znacznie wykraczający swoim zakresem poza granice pojedynczego przedsiębiorstwa. Z tego względu niezwykle istotne staje się opracowanie i wdrożenie spójnej architektury integracyjnej, która w ramach wspólnego środowiska przetwarzania w sposób kompleksowy odzwierciedlałaby reguły integracji organizacji oraz zasady jej współpracy z podmiotami zewnętrznymi. Opracowywanie założeń nowej architektury integracyjnej powinno uwzględniać podejście procesowe[6].

---

[2] Przy pisaniu tego artykułu autor korzystał z treści zamieszczonych w monografii: S.J. Rysz, *Zarządzanie kryzysowe zintegrowane*, Warszawa 2016.

[3] Por. tamże, s. 177–185.

[4] Na przykład podmioty komercyjne świadczące usługi ratownictwa medycznego.

[5] Trzeci sektor to wszystkie formy działań społecznych mieszczące się pomiędzy państwem a rynkiem, http://fakty.ngo.pl/trzeci-sektor (dostęp: 20.10.2016 r.).

[6] Por. A. Niesler, *Integracja systemów informatycznych przedsiębiorstwa w architekturze z autonomicznym rejestrem usług sieciowych*, http://www.dbc.wroc.pl/Content/15602/Niesler_Integracja_systemow_informatycznych_przedsiebiorstwa_w_architekturze.pdf (dostęp: 17.10.2016 r.).

System informatyczny wykorzystywany do integracji środowiska zarządzania kryzysowego musi spełniać kilka wymagań: musi być wydajny, wielodziedzinowy[7], stabilny, ekskluzywny[8], odporny na zagrożenia pochodzące zarówno z przestrzeni realnej, jak i z przestrzeni wirtualnej[9] (cyberprzestrzeni) oraz dostępny dla wszystkich uczestników systemu zarządzania kryzysowego. Dla uzyskania optymalizacji procesu zarządzania kryzysowego konieczne jest, żeby taki wspomagający ów proces zintegrowany system informatyczny:

- odzwierciedlał strukturę zależności i podległości w strukturze systemu zarządzania kryzysowego;
- odzwierciedlał w czasie rzeczywistym dostępność zasobów koniecznych do realizacji zadań zarządzania kryzysowego;
- umożliwiał monitoring zmian wartości czynników kluczowych z punktu widzenia materializacji wybranych, najistotniejszych zagrożeń;
- na bieżąco, poprzez wprowadzanie zachodzących zmian aktualizował stan środowiska, którego dotyczy[10];
- umożliwiał symulowanie skutków proponowanych decyzji oraz prognoz przebiegu sytuacji z uwzględnieniem stanu środowiska oraz zadawanych w nim incydentów[11];
- pozwalał na automatyzację wybranych procesów[12].

Integrowanie sytemu zarządzania kryzysowego z użyciem technologii informatycznej ma dodatkowe uzasadnienie, które wynika z jego opartej na procesach struktury. Pod pojęciem procesu rozumieć należy zestawienie kolejnych czynności wzajemnie ze sobą powiązanych w łańcuch przyczynowo-skutkowy, w którym zakończenie czynności poprzedniej stanowi przyczynę do uruchomienia następnej, które prowadzą do wytworzenia rezultatu będącego efektem zrealizowania procesu jako całości. Trzeba rozróżnić procesy charakterystyczne dla osiągania zaplanowanego celu[13] organizacji od procesów pomocniczych, niezbędnych do jej standardowego funkcjonowania. Wśród procesów pomocniczych znajdą się te, które wiążą się z zarządzaniem jednostką, obsługą pracowników, urzędów i biur.

---

[7] Wielość dziedzin, jakie muszą być uwzględniane w takim zintegrowanym systemie informatycznym do obsługi procesu zarządzania kryzysowego wynika z charakteru samego procesu i mnogości obszarów, których dotyczy.

[8] Ekskluzja – wykluczenie, odrzucenie. W rozważanym odniesieniu słowo „ekskluzywny" występuje w znaczeniu: zamknięty, z dostępem ograniczonym i reglamentowanym tylko dla tych, którzy uzyskają odpowiednie uprawnienia. Opracowano na podstawie: http://sjp.pwn.pl/slowniki/ekskluzja.html oraz http://sjp.pwn.pl/sjp/ekskluzywny;2456503.html (dostęp: 18.10.2016 r.).

[9] Por. S.J. Rysz, *Zarządzanie kryzysowe zintegrowane...*, s. 294–296.

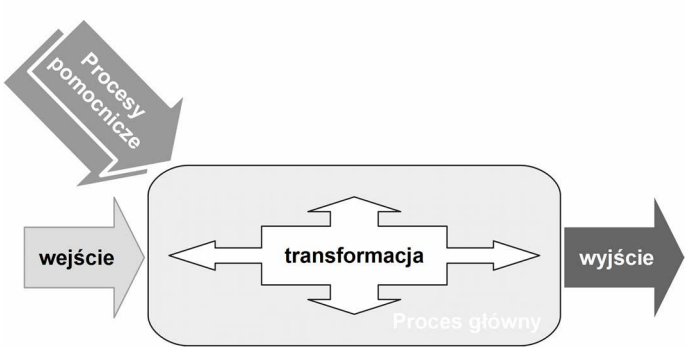
[10] Autor ma tu na myśli bieżącą aktualizację monitorowanych parametrów, ale także wprowadzanie zmian prawnych, personalnych, adresowych, kontaktowych itp.

[11] Słowo „incydent" odzwierciedla tu akt negatywnej zmiany, który może zaistnieć w rozważanym środowisku.

[12] Chodzi tu przede wszystkim o raportowanie sytuacji według założonego algorytmu.

[13] Dużym problemem w przypadku informatyzacji procesów administracji publicznej jest brak precyzji w formułowaniu celów. Por. J. Sasak i A.J. Kożuch, *Modelowanie procesów organizacyjnych jako narzędzie integracji systemów informatycznych administracji publicznej*, „Współczesne Zarządzanie", 3/2011, artykuł otwarty na stronie: http://8723.indexcopernicus.com/fulltxt.php?ICID=1063271. (dostęp: 8.02.2017 r.).

Na rysunku 1 pokazano ideę procesu, zaś w tabeli 1 ukazanych zostało 13 wybranych procesów, które są realizowane na każdym[14] szczeblu systemu zarządzania kryzysowego. Dla każdego z nich wskazano dane wejściowe oraz dane wyjściowe oraz określono fazę[15] procesu zarządzania kryzysowego, której ów proces dotyczy[16].



Rys. 1. Graficzne zobrazowanie sposobu kreowania subiektywnego poczucia bezpieczeństwa uwarunkowanego na bazie obiektywnego stanu bezpieczeństwa w rozważanym środowisku.

Źródło: S.J. Rysz, *Zarządzanie kryzysowe zintegrowane*..., s. 145.

Tabela 1. Przykładowe zestawienie wybranych procesów realizowanych w ramach zarządzania kryzysowego.

Lp.	Wejście procesu	Proces	Wyjście procesu	Uwagi
1	Wartości mierzonych parametrów	**Monitoring**	Obraz sytuacji	Wszystkie fazy zarządzania kryzysowego (ZK)
2	Decyzja	**Ostrzeganie i alarmowanie**	Sygnały i komunikaty ostrzegawcze i alarmowe	Faza przygotowania
3	Obraz sytuacji	**Powiadamianie i informowanie**	Komunikat	Faza przygotowania i reagowania
4	Informacja o zdarzeniu kryzysowym	**Powiadamianie ratunkowe**	Akcja służb, straży i podmiotów ratunkowych	W każdych warunkowych
5	Dane bieżące i archiwalne	**Prognozowanie**	Pakiet możliwych wariantów rozwoju sytuacji	We wszystkich fazach ZK

[14] Algorytm procesu jest dostosowany do szczebla systemu zarządzania kryzysowego i odzwierciedla jego udział w procedurach.

[15] W literaturze przedmiotu zarządzanie kryzysowe w odniesieniu do konkretnych zagrożeń dzieli się na cztery następujące po sobie fazy. Są to: „zapobieganie", „przygotowanie", „reagowanie" oraz „odbudowa". Opracowano na podstawie: S.J. Rysz, *Zarządzanie kryzysowe zintegrowane...*, s. 58–71.

[16] Por. E. Ziemba, I. Obłąk, *Systemy informatyczne w organizacjach zorientowanych procesowo*, https://pz.wz.uw.edu.pl/sites/default/files/artykuly/ziemba_oblak.pdf (dostęp: 19.10.2016 r.).

6	Dane bieżące i prognozy rozwoju sytuacji	**Symulowanie**	Wirtualna sekwencja możliwych zdarzeń i ich ewentualnych skutków	We wszystkich fazach ZK
7	Dane o sytuacji, dane o dostępnych zasobach, prognozy, symulacje, opinie ekspertów	**Decydowanie**	Postanowienia co do zakresu użytych zasobów i sposobu ich użycia	We wszystkich fazach ZK
8	Dane o sytuacji i zasobach	**Raportowanie**	Sformalizowana informacja przekazana poziomowi nadrzędnemu	We wszystkich fazach ZK
9	Dane o zasobach i potrzebach	**Planowanie**	Dokumenty planistyczne, harmonogramy i programy działania	Faza zapobieganie i przygotowanie
10	Dane o zasobach	**Przygotowanie**	Uzupełnianie zapasów magazynowych i sprzętowych, szkolenie ratowników i akcja edukacyjna wśród ludności, ostrzeżenia dla ludności	Faza przygotowanie
11	Wezwanie, zgłoszenie alarmowe, decyzja	**Reagowanie**	Działania służb, straży i inspekcji oraz innych właściwych podmiotów w akcji ratunkowej	Faza reagowanie
12	Protokoły, zdjęcia, raporty	**Szacowanie skutków**	Protokoły zweryfikowanych strat	Faza odbudowa
13	Plany, projekty	**Odbudowa i odtwarzanie**	Odbudowane obiekty odtworzona funkcjonalność infrastruktury	Faza odbudowa

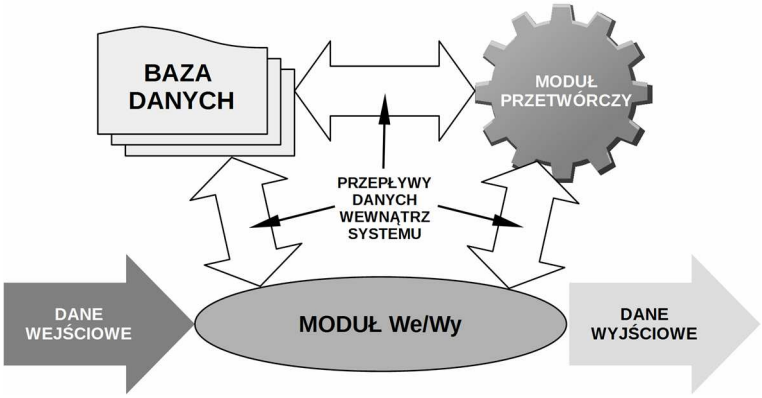
Źródło: tamże, s. 146–147.

W sposób intuicyjny taki zintegrowany informatyczny system można przedstawić jako pakiet trzech współpracujących ze sobą elementów:

1. modułu wejścia/ wyjścia, który ma za zadanie umożliwić wprowadzanie do systemu danych szczegółowych charakterystycznych dla zasobu lub wybranego elementu systemu zarządzania kryzysowego;
2. modułu bazy danych, w której gromadzone są i przechowywane pozyskane dane oraz wyniki przeprowadzanych na nich operacji;
3. modułu przetwórczego, który umożliwia transformowanie – według zadanych algorytmów – pozyskanych danych wejściowych na dane wyjściowe (analizy, raporty, statystyki, wykresy itp.) potrzebne dla optymalnej oceny przebiegu zdarzeń i podejmowania najlepszych w tej sytuacji decyzji.

Wewnątrz systemu, pomiędzy jego modułami następuje ustawiczna wymiana danych realizowana za pomocą infrastruktury składającej się z urządzeń i aplikacji oraz sieci ich wzajemnych połączeń. Danymi wejściowymi mogą być zarówno pobierane automatycznie wskazania czujników monitorujących newralgiczne z punktu widzenia zarządzania kryzysowego parametry środowiska, jak i dane wprowadzane przez operatora z klawiatury komputera podłączonego do zintegrowanego systemu informatycznego.

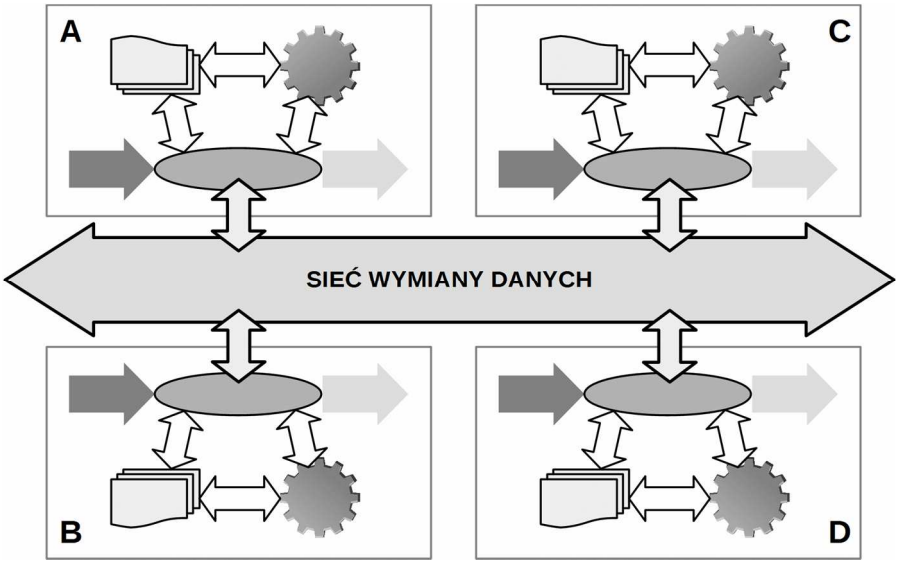
Rys. 2 przedstawia najprostszy i wyidealizowanych model informatycznego systemu zintegrowanego. W rzeczywistych warunkach sytuacja jest bardziej skomplikowana, choć nie oznacza to wcale, że niemożliwa do integracji wokół systemu informatycznego. Model na rys. 3 lepiej odzwierciedla rzeczywistą specyfikę środowiska informatycznego właściwego dla struktury podmiotów uczestniczących w procesie zarządzania kryzysowego.



Rys. 2. Graficzne zobrazowanie idei działania zintegrowanego systemu informatycznego
Źródło: opracowanie własne.

Każdy z osobnych ekskluzywnych zintegrowanych systemów informatycznych funkcjonuje w oparciu o dane wejściowe właściwe dla poszczególnych posługujących się nimi podmiotów oznaczonych na rys. 3 odpowiednio: A, B, C i D. Ich wzajemne komunikowanie się i ewentualna współpraca możliwa jest z wykorzystaniem sieci wymiany danych. Może to być zarówno ogólnodostępna sieć Internet, jak i specjalnie w tym celu przygotowane łącza dziedzinowe, na przykład Ogólnopolska Sieć Teleinformatyczna Na Potrzeby Numeru 112[17] – OST 112.

[17] W latach 2015–2020 zaplanowana została rozbudowa sieci OST 112, która umożliwi włączenie do niej oprócz podmiotów Systemu Powiadamiania Ratunkowego, Policji, Państwowej Straży Pożarnej i skoncentrowanych dyspozytorni Systemu Państwowe Ratownictwo Medyczne, także całej administracji publicznej. Opracowano na podstawie odpowiedzi z dnia 10.04.2015 r. na interpelację nr 31630 w sprawie realizacji projektu „Ogólnopolska sieć teleinformatyczna na potrzeby obsługi numeru alarmowego 112" ze strony: http://www.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=2E6A4613 (dostęp: 18.10.2016 r.).



Rys. 3. Graficzne zobrazowanie struktury teleinformatycznego środowiska i współdziałania ekskluzywnych zintegrowanych systemów informatycznych

Źródło: opracowanie własne.

		SEGMENT			
		decyzyjny	doradczy opiniotwórczy	organizacyjny	ratowniczy interwencyjny
POZIOM					
krajowy	ADMINISTRACJA RZĄDOWA	Rada Ministrów Prezes RM	Rządowy Zespół Zarządzania Kryzysowego	Rządowe Centrum Bezpieczeństwa	Centralne zasoby ratownicze i interwencyjne
resortowy	ADMINISTRACJA RZĄDOWA	Minister kierujący działem administracji rządowej / Kierownik urzędu centralnego	Zespół Zarządzania Kryzysowego ministerstwa / urzędu centralnego	Centrum Zarządzania Kryzysowego ministerstwa / urzędu centralnego	Resortowe zasoby ratownicze i interwencyjne
wojewódzki	ADMINISTRACJA RZĄDOWA	WOJEWODA	Wojewódzki Zespół Zarządzania Kryzysowego	Wojewódzkie Centrum Zarządzania Kryzysowego	Wojewódzkie zasoby ratownicze i interwencyjne
powiatowy	ADMINISTRACJA SAMORZĄDOWA	Starosta Prezydent miasta	Powiatowy Zespół Zarządzania Kryzysowego	Powiatowe Centrum Zarządzania Kryzysowego	Powiatowe zasoby ratownicze i interwencyjne
gminny (miejski)	ADMINISTRACJA SAMORZĄDOWA	Wójt Burmistrz Prezydent miasta	Gminny (Miejski) Zespół Zarządzania Kryzysowego	Gminne (Miejskie) Centrum Zarządzania Kryzysowego	Gminne zasoby ratownicze i interwencyjne

Rys. 4. Schemat blokowy struktury organizacyjnej systemu zarządzania kryzysowego w Polsce

Źródło: S.J. Rysz, *Zarządzanie kryzysowe zintegrowane*..., s. 55.

Z punktu widzenia blokowego schematu systemu zarządzania kryzysowego w województwach, jego organizacyjna struktura (rys. 4) wynika z zapisów ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[18] i jest zunifikowana i powtarzalna. Różnice szczegółowe wynikają z warunków lokalnych. System ten opiera się na administracji publicznej[19] – samorządowej i rządowej – począwszy od szczebla gminnego, a na centralnym skończywszy.

Największymi elementami tego systemu są województwa, które stanowią najniższy poziom zaangażowania administracji rządowej. U podstaw systemu jest samorząd gminny. Powiat, ze względu na struktury organizacyjne Policji i Państwowej Straży Pożarnej jest szczeblem kluczowym z punktu widzenia reagowania kryzysowego[20].

3. INTEGRACJA EKSKLUZYWNA (CENTRALNA)

Zdawać by się mogło, że najprostszym podejściem byłoby zorganizowanie zintegrowanego informatycznego systemu ekskluzywnego w rodzaju tego, który został przedstawiony na rysunku 1. Byłby to mechanizm w pełni dedykowany dla rozważanego procesu zarządzania kryzysowego, odzwierciedlający strukturę całego systemu i dopuszczający do jego użytkowania jedynie uczestniczące w nim podmioty[21].

Analiza SWOT[22] pozwoli lepiej poznać wady i zalety tak zaplanowanego systemu.

- Mocne strony:
  a) rozbudowana struktura modułu WE/WY – dane wejściowe przekazywane bezpośrednio do centralnej bazy danych;
  b) rozbudowana centralna baza danych;
  c) rozbudowany centralny moduł obliczeniowy;
  d) transmisja po specjalnie w tym celu wydzielonych teleinformatycznych łączach ogólnokrajowych[23];
  e) jednolita struktura danych w całym kraju;
  f) unifikacja w skali całego kraju sposobu pracy poszczególnych podmiotów współpracujących z systemem;
  g) standaryzacja współpracujących z systemem zasobów teleinformatycznych.
- Słabe strony:
  a) konieczność tworzenia dużych kopii bezpieczeństwa systemu;
  b) większa podatność systemu na agresję fizyczną i cyberagresję[24];
  c) konieczność przetwarzania dużych zbiorów danych;

[18] Tekst jedn. Dz.U. z 2017 r., poz. 209.
[19] Por. tamże, art. 2.
[20] Por. S.J. Rysz, *Zarządzanie kryzysowe zintegrowane*..., s. 303–306.
[21] Takie założenie dotyczy ustawicznego korzystania z systemu i zasobów. Oczywiście w sytuacjach szczególnych system może być udostępniany innym doraźnie upoważnionym podmiotom przy zachowaniu koniecznych standardów bezpieczeństwa.
[22] SWOT – akronim angielskich słów: *strengths* – mocne strony, *weaknesses* – słabe strony, *opportunities* – szanse oraz *threats* – zagrożenia.
[23] Na przykład po sieci OST 112.
[24] Słowem: „cyberagresja" określa się tu wszystkie formy ataku na zasoby systemu dokonywane z przestrzeni wirtualnej – cyberprzestrzeni.

d) utrata danych może powodować paraliż decyzyjny w całym kraju;
e) konieczność centralnego zarządzania bazą uczestników upoważnionych do podejmowania aktywności w systemie;
f) zagrożenie utraty nadzoru nad sytuacją w kraju w wyniku awarii systemu;
g) większe zagrożenie przypadkowego lub celowego zainfekowania systemu;
h) kumulacja kosztów budowy i obsługi systemu na poziomie centralnym;
i) duża energochłonność systemu – konieczność poniesienia dużych nakładów na przygotowanie odpowiedniego obiektu i infrastruktury instalacyjnej.

- Szanse:
  a) postęp technologiczny w informatyce i telekomunikacji, który sprawi, że:
     I. wzrośnie wydajność i sprawność urządzeń i aplikacji;
     II. zmniejszą się koszty ich zakupu i użytkowania;
  b) możliwość wspierania działań w terenie z poziomu centralnego;
  c) poprawa wykształcenia informatycznego absolwentów studiów na kierunkach związanych z bezpieczeństwem.
- Zagrożenia:
  a) postęp technologiczny w informatyce i telekomunikacji – to, co zostało wskazane jako szansa jest jednocześnie zagrożeniem dla ekskluzywnego zintegrowanego systemu informatycznego. Ten sam postęp przełoży się także na alternatywne sposoby integracji;
  b) duże koszty utrzymania rozbudowanego centralnego systemu informatycznego;
  c) zależność od podmiotów zajmujących się konserwacją i obsługą systemu;
  d) zapędy w kierunku centralnego sterowania działaniami w terenie;
  e) większe prawdopodobieństwo pomyłki przy ustalaniu poziomów dostępowych dla dużej rzeszy pracowników z całego kraju.

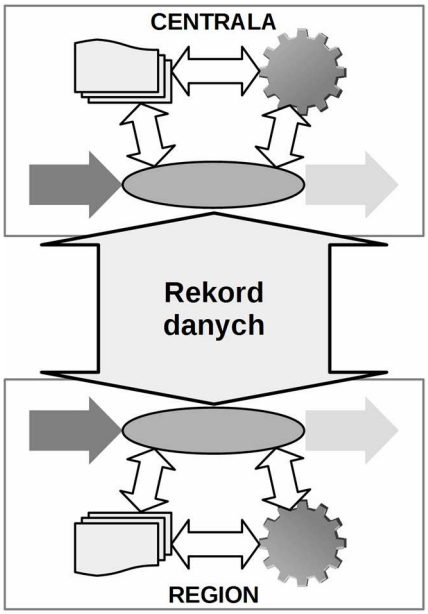
4. INTEGRACJA INKLUZYJNA (HYBRYDOWA)

Alternatywą dla takiego centralnego zintegrowanego systemu informatycznego jest system inkluzyjny[25], działający w oparciu o regionalne systemy zintegrowane w poszczególnych województwach (rys. 5).

Specyfika takiego sposobu informatycznego zintegrowania systemu zarządzania kryzysowego w Polsce zakłada utworzenie nadrzędnego systemu centralnego (swoistej centralnej nakładki systemowej), który byłby zasilany potrzebnymi mu danymi przez regionalne systemy funkcjonujące w poszczególnych województwach (hybrydowa[26] struktura rozproszonych zasobów regionalnych). Zaletą takiego podejścia do zagadnienia jest zachowanie już zrealizowanych systemów. Ich współpraca z systemem centralnym mogłaby się odbywać za sprawą odpowiednio przygotowanych interfejsów obsługujących jeden wspólny dla wszystkich rekord danych.

[25] Inkluzja – włączenie czegoś lub kogoś w większą całość. Opracowano na podstawie: http://sjp.pl/inkluzja (dostęp: 18.10.2016 r.).

[26] Słowo „hybrydowa" odnosi się w tym przypadku do możliwej różnorodności składników systemu informatycznego. Wymiana danych pomiędzy lokalnie zintegrowanymi składnikami systemu docelowego za pośrednictwem jednolitego rekordu wymaga jedynie zestawienia w punktach styku odpowiednich interfejsów.



Rys 5. Schemat blokowy struktury inkluzyjnego zintegrowanego systemu informatycznego
Źródło: opracowanie własne.

Dla porównania analiza SWOT takiego systemu przedstawia się następująco:

- Mocne strony:
  a) łatwiejsze wdrożenie takiego systemu z uwagi na oparcie jego działania na już działających w województwach zintegrowanych systemach informatycznych,
  b) system centralny kompiluje dane w wymiarze potrzebnym jedynie do stworzenia obrazu sytuacji w kraju,
  c) dywersyfikacja miejsc przechowywania danych – dane do zobrazowania stanu procesu zarządzania kryzysowego w kraju są w bazach regionalnych przechowywane w formie cząstkowej oraz w formie skumulowanej w bazie centralnej,
  d) dywersyfikacja kosztów budowy systemu,
  e) mniejsze ilości danych przesyłanych pomiędzy systemami regionalnymi oraz systemem centralnym,
  f) mniejsze objętości baz danych,
  g) mniejsze objętości kopii zapasowych,
  h) awaria systemu centralnego nie unieruchamia systemów regionalnych,
  i) awaria pojedynczego systemu regionalnego nie unieruchamia systemu centralnego ani pozostałych systemów regionalnych,
  j) większa odporność systemu na akty agresji z przestrzeni realnej i wirtualnej,
  k) łatwiejsze odtwarzanie zasobów w każdym elemencie systemu po ewentualnej awarii lokalnej,

- Słabe strony:
  a) obraz sytuacji w kraju wynikający z przekazywanych z ośrodków regionalnych danych – wojewódzkich centr zarządzania kryzysowego,
  b) dynamika zmian obrazu sytuacji zależna od aktywności poszczególnych ośrodków regionalnych.
- Szanse:
  a) postęp technologiczny w informatyce i telekomunikacji, który sprawi, że:
     I. wzrośnie wydajność i sprawność urządzeń i aplikacji;
     II. zmniejszą się koszty ich zakupu i użytkowania.
  b) poprawa jakości kształcenia studentów na kierunkach związanych z bezpieczeństwem,
- Zagrożenia:
  a) podjęcie na szczeblu centralnym decyzji i działań zmierzających do stworzenia struktury ogólnokrajowej w formie wyżej opisanego systemu ekskluzywnego.

5. INTEGRACJA SYSTEMÓW REGIONALNYCH W WOJEWÓDZTWACH

Przygotowanie zintegrowanego systemu zarządzania kryzysowego właściwego dla konkretnego województwa i działających na jego obszarze podmiotów należy zacząć od audytu zasobów oraz obowiązujących zasad i procedur gospodarowania nimi.

Poniżej przedstawiono przykład[27] analizy SWOT systemu.

- Do mocnych stron można zaliczyć:
  a) istniejącą i planowaną infrastrukturę lokalnych inicjatyw samorządowych,
  b) dbałość mieszkańców o swoje zagrody i ich otoczenie,
  c) istniejące i funkcjonujące systemy SWO i SWA,
  d) doświadczenie, wiedzę i umiejętności służb zajmujących się reagowaniem kryzysowym,
  e) doświadczenie osób i służb w zakresie podejmowania decyzji i działań, które jest skutkiem cyklicznie powtarzających się zdarzeń kryzysowych,
  f) dostępne zasoby rzeczowe i teleinformatyczne w poszczególnych podmiotach,
  g) dobry stan infrastruktury publicznej,
  h) dobrą współpracę organów administracji publicznej między sobą oraz z podmiotami i obywatelami na zarządzanym terenie,
  i) sprawny system realizujący wsparcie państwa dla poszkodowanych w wyniku zdarzeń powodziowych, osuwiskowych i innych,
  j) system ubezpieczeń majątkowych.
- Jako słabe strony można wskazać:
  a) brak bezpiecznych miejsc parkingowych dla samochodów transportujących niebezpieczne środki chemiczne,
  b) brak bezpiecznych bocznic kolejowych dla składów kolejowych przewożących niebezpieczne środki chemiczne,
  c) niedostateczną wielkość rezerw na zarządzanie kryzysowe planowanych w budżetach niektórych samorządów,

[27] Opracowano na podstawie: S.J. Rysz, *Zarządzanie kryzysowe zintegrowane...*, s. 291-292.

d) podejmowanie działań zarządzania kryzysowego dopiero w chwili wystąpienia sytuacji kryzysowej, incydentalnie i doraźnie, bez właściwego długofalowego przygotowania i aprowizacji,
e) specyfikę obszaru (klimat, sieć rzek i cieków, sieć szlaków komunikacyjnych, budowa geologiczna, ukształtowanie terenu i sposób jego zagospodarowania) sprzyjającą dynamicznym powodziom o charakterze górskim oraz osuwiskom,
f) systemy SWA i SWO oparte o stare technologie i urządzenia (zbyt mało syren elektronicznych, które umożliwiają nadawanie komunikatów słownych),
g) politykę prowadzenia zabudowy mieszkaniowej i komercyjnej na terenach zagrożonych (np. zalewowych lub osuwiskowych),
h) brak powszechności ubezpieczeń od niekorzystnych zdarzeń wśród obywateli.

- Do szans można zaliczyć:
  a) postęp technologiczny i organizacyjny działań ratowniczych,
  b) stosowanie coraz nowszych technologii,
  c) względne obniżanie cen sprzętu do ostrzegania i alarmowania,
  d) prowadzenie prac realizujących zapisy dyrektyw przeciwpowodziowych[28] oraz środki UE udostępnione do prowadzenia wynikających z nich inwestycji powinny doprowadzić do uporządkowania przestrzeni nad rzekami i ciekami wodnymi,
  e) postęp w myśleniu obywateli o zagrożeniach, który pozwala podejmować inicjatywy zmierzające do usprawnienia akcji ratunkowej oraz do ograniczania skutków zdarzeń w razie ich materializacji,
  f) lokalne inicjatywy mieszkańców i samorządów na rzecz podnoszenia poziomu bezpieczeństwa w miejscu zamieszkania i codziennej pracy.
- Wśród zagrożeń można wskazać:
  a) bierne czekanie obywateli na pomoc ze strony państwa;
  b) pomoc państwa nie jest powiązana z trwałą likwidacją zagrożenia zdarzeniem, które powodują okoliczności skutkujące udzielaniem pomocy (zalane domy są remontowane i pozostają w dalszym ciągu w obszarze zalewowym);
  c) komunikaty niezwiązane z ostrzeganiem o zagrożeniach wysyłane w systemach sms przeznaczonych do ostrzegania i alarmowania;
  d) brak rozwiązań prawnych ograniczających zabudowę na terenach zalewowych i osuwiskowych.

6. PODSUMOWANIE

Specyfika zarządzania kryzysowego polega w dużej mierze na poszukiwaniu możliwości ograniczania skutków zdiagnozowanych zagrożeń oraz na podążaniu z akcjami reagowania do miejsc ich materializacji. Idąc dalej w tych rozważaniach trzeba dostrzec, że pakietowość występujących zagrożeń[29], ich nieprzewidywalność zarówno co do charakteru,

[28] Autor ma tu na myśli w pierwszej kolejności obowiązek sporządzenia map zagrożenia powodziowego oraz ryzyka powodziowego przypisanych do obszaru województwa.

[29] Zagrożenia prawie zawsze materializują się w pakietach. Zwykle są to zestawy powtarzalne. Na przykład „opady nawalne, powodzie i osuwiska". Szerzej o tym w S.J. Rysz, *Zarządzanie kryzysowe zintegrowane...*, s. 24–33.

jak i co do skali sprawiają, że koszty działań zawsze przerastają zaplanowane na ich realizację środki budżetowe. Trzeba więc szukać sposobów, żeby ta dysproporcja była jak najmniejsza. Służyć temu mogą informatyczne systemy integrujące zasoby procesu zarządzania kryzysowego.

Każdy z przedstawionych powyżej typów integracji, zarówno ekskluzywny (scentralizowany), jak i inkluzyjny (hybrydowy) oraz wszystkie systemy regionalne wymagają odpowiedzialnego organizowania uczestnictwa podmiotów w systemie. Ze względu na istotę systemu i gromadzone w nim zasoby, dostęp do niego musi być reglamentowany w strukturze szczeblowej (poziomowej), która pozwala precyzyjnie organizować i dzielić uprawnienia.

Nie jest celem niniejszego opracowania wskazywać, który z systemów jest lepszy do stosowania. Należy jednak wskazać na istotny szczegół, który dotyczy obu z omawianych systemów nadrzędnych: każdy z nich inaczej odnosi się do obecnie funkcjonujących systemów regionalnych. System ekskluzywny będzie je zastępować, w wyniku czego staną się niepotrzebne i będą marginalizowane. To może spowodować problemy z rozliczaniem środków, za które w niektórych województwach takie systemy były budowane[30]. Poza tym zostanie zaprzepaszczony entuzjazm, wiedza i doświadczenie osób, które takie systemy tworzyły. Te wartości wnoszą istotny efekt synergetyczny do działania systemu zarządzania kryzysowego i byłoby poważnym błędem, gdyby ich nie brać pod uwagę.

Przytoczone powyżej zastrzeżenia nie występują przy systemie inkluzyjnym. Byłby on realizowany z istotnym wykorzystaniem elementów już funkcjonujących, jednocześnie zachowując ich odrębność i cechy, które czynią go odpowiednim dla regionalnych zastosowań.

LITERATURA

[1] Niesler A., *Integracja systemów informatycznych przedsiębiorstwa w architekturze z autonomicznym rejestrem usług sieciowych*, http://www.dbc.wroc.pl/Content/15602/Niesler_Integracja_systemow_informatycznych_przedsiebiorstwa_w_architekturze.pdf (dostęp: 17.10.2016 r.).

[2] Rysz S.J., *Zarządzanie kryzysowe zintegrowane*, Difin S.A., Warszawa 2016.

[3] Sasak J., Kożuch A.J., *Modelowanie procesów organizacyjnych jako narzędzie integracji systemów informatycznych administracji publicznej*, http://8723.indexcopernicus.com/fulltxt.php?ICID=1063271 (dostęp: 8.02.2017 r.).

[4] Ziemba E., Obłąk I., *Systemy informatyczne w organizacjach zorientowanych procesowo*, https://pz.wz.uw.edu.pl/sites/default/files/artykuly/ziemba_oblak.pdf (dostęp: 19.10.2016 r.).

[5] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jedn. Dz.U. z 2017 r., poz. 209).

[6] http://fakty.ngo.pl/trzeci-sektor (dostęp: 20.10.2016 r.).

[7] http://sjp.pl/inkluzja (dostęp: 18.10.2016 r.).

[8] http://sjp.pwn.pl/sjp/ekskluzywny;2456503.html (dostęp: 18.10.2016 r.).

[30] Środki na budowę takich systemów mogły pochodzić z funduszy strukturalnych Unii Europejskiej. Takie projekty do właściwego rozliczenia wymagają spełnienia – między innymi – warunku trwałości, który w odniesieniu do rozważanych zagadnień, w najprostszej formie polega na minimalnym kilkuletnim okresie ich funkcjonowania.

[9] http://sjp.pwn.pl/slowniki/ekskluzja.html (dostęp: 18.10.2016 r.).
[10] http://www.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=2E6A4613 (dostęp: 18.10. 2016 r.).

INTEGRATION BASED ON INFORMATICS IN THE AREA OF CRISIS MANAGEMENT

Crisis management in a large part it is searching for possibilities to reduce effects of diagnosed hazards and also to reach with the activities to places where they will materialized. Going further in these considerations one needs to see that existing threats usually are in bundle and they are unpredictably both as to the nature and to the scale. It makes that costs of actions always overwhelm resources scheduled for their realization. It is, therefore, necessary to seek for ways that this disproportion would be as small as possible. Informatics systems for integration are very suitable for that process. Environmental of entities participating in the crisis management system in Poland is a hybrid cluster. Such specificity of participants makes the system vulnerable to difficulties in reconciling the particular interests of individual entities, which can make it difficult to achieve optimum efficiency and effectiveness. Due to the importance the availability and flow of information in the process of crisis management, it is expected that the implementation of informatics technology, tools and procedures for integrating environment can have a positive impact to minimize such risks. The idea is to organize cooperation in the environment of crisis management system participants through the use of resources and ICT (hardware, application, network, and personnel) to efficiently obtain necessary data for the proper assessment of the situation of events, availability and consumption of resources and inventories and planning and carrying out actions in crisis situations.

Keywords: crisis management, integration, efficiency, effectiveness.

DOI: 10.7862/rz.2017.mmr.20

Tekst złożono w redakcji: grudzień 2016 r.
Przyjęto do druku: czerwiec 2017 r.